

Exhibit A--Summons and Complaint

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ROCKLAND COUNTY**

-----X
REBECCA KRANDLE, individually, and on behalf of all
others similarly situated,

Plaintiff/Petitioner,

- against -

Index No.032188/2022

REFUAH HEALTH CENTER, INC.,

Defendant/Respondent.
-----X

**NOTICE OF ELECTRONIC FILING
(Mandatory Case)
(Uniform Rule § 202.5-bb)**

You have received this Notice because:

- 1) The Plaintiff/Petitioner, whose name is listed above, has filed this case using the New York State Courts E-filing system ("NYSCEF"), and
- 2) You are a Defendant/Respondent (a party) in this case.

● **If you are represented by an attorney:**

Give this Notice to your attorney. (Attorneys: see "Information for Attorneys" pg. 2).

● **If you are not represented by an attorney:**

You will be served with all documents in paper and you must serve and file your documents in paper, unless you choose to participate in e-filing.

If you choose to participate in e-filing, you must have access to a computer and a scanner or other device to convert documents into electronic format, a connection to the internet, and an e-mail address to receive service of documents.

The **benefits of participating in e-filing** include:

- serving and filing your documents electronically
- free access to view and print your e-filed documents
- limiting your number of trips to the courthouse
- paying any court fees on-line (credit card needed)

To register for e-filing or for more information about how e-filing works:

- visit: www.nycourts.gov/efile-unrepresented or
- contact the Clerk's Office or Help Center at the court where the case was filed. Court contact information can be found at www.nycourts.gov

To find legal information to help you represent yourself visit www.nycourthelp.gov

**Information for Attorneys
(E-filing is Mandatory for Attorneys)**

An attorney representing a party who is served with this notice must either:

1) immediately record his or her representation within the e-filed matter on the NYSCEF site www.nycourts.gov/efile ; or

2) file the Notice of Opt-Out form with the clerk of the court where this action is pending and serve on all parties. Exemptions from mandatory e-filing are limited to attorneys who certify in good faith that they lack the computer hardware and/or scanner and/or internet connection or that they lack (along with all employees subject to their direction) the knowledge to operate such equipment. [Section 202.5-bb(e)]

For additional information about electronic filing and to create a NYSCEF account, visit the NYSCEF website at www.nycourts.gov/efile or contact the NYSCEF Resource Center (phone: 646-386-3033; e-mail: nyscef@nycourts.gov).

Dated: May 18, 2022

Michael Liskow

Name

Calcaterra Pollack LLP

Firm Name

1140 Avenue of the Americas, 9th Floor
Address

New York, NY 10036-5803

(212) 899-1761

Phone

mliskow@calcaterrapollack.com

E-Mail

To: Refuah Health Center, Inc.

728 N. Main Street

Spring Valley, NY 10977

FILED: ROCKLAND COUNTY CLERK 05/17/2022 04:50 PM

INDEX NO. 032188/2022

NYSCEF DOC. NO. 1

RECEIVED NYSCEF: 05/17/2022

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ROCKLAND**REBECCA KRANDLE, individually, and on
behalf of all others similarly situated,

Index No:

Plaintiff,

SUMMONS

v.

REFUAH HEALTH CENTER, INC.,

Defendant.

To the above-named Defendant:

You are hereby summoned and required to serve upon plaintiff's attorneys an answer to the Complaint in this action within twenty days after the service of this summons, exclusive of the day of service, or within thirty days after service is complete if this summons is not personally delivered to you within the State of New York. In the case of your failure to answer, judgment will be taken against you by default for the relief demanded in the Complaint.

Plaintiff designates Rockland County as the place of trial. The basis of venue is defendant Refuah Health Center, Inc.'s principal place of business in this County, which is .

Dated: West Orange, New Jersey
May 17, 2022

Michael Liskow

Michael Liskow
Calcaterra Pollack, LLP
1140 Avenue of the Americas, 9th Floor
New York, NY 10036-5803
Tel: (212) 899-1761
Fax: (332) 206-2073
mliskow@calcaterrapollack.com

To: REFUAH HEALTH CENTER, INC.

**SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF ROCKLAND**

REBECCA KRANDLE, individually, and
on behalf of all others similarly situated,

Plaintiff,

v.

REFUAH HEALTH CENTER, INC.,

Defendant.

Case No.

CLASS ACTION
JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Rebecca Krandle (“Plaintiff”), individually, and on behalf of all others similarly situated (collectively, “Class members”), by and through her attorneys, brings this Class Action Complaint against Refuah Health Center, Inc. (“RHC”) and complains and alleges upon personal knowledge as to herself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against RHC for its failure to secure and safeguard her and approximately 260,740 other individuals’ personally identifying information (“PII”) and personal health information (“PHI”), including names, Social Security numbers, driver’s license numbers, state identification numbers, dates of birth, bank/financial account information, credit/debit card information, medical treatment/diagnosis information, Medicare/Medicaid numbers, medical record numbers, patient account numbers, and/or health insurance policy numbers.

2. RHC is a healthcare company with its principal place of business in Spring Valley, New York. RHC has locations in Spring Valley and South Fallsburg, New York. RHC is a not-for-profit company formed in New York in 1992.

3. Between May 31, 2021 and June 1, 2021, unauthorized individuals gained access to RHC's network systems and accessed and acquired files from the system that contained the PII/PHI of Plaintiff and Class members (the "Data Breach").

4. RHC owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. RHC breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its patients' and former patients' PII/PHI from unauthorized access and disclosure.

5. As a result of RHC's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of herself and all persons whose PII/PHI was exposed as a result of the Data Breach, which RHC first publicly acknowledged on or about April 29, 2022, over ten months after the breach occurred.

6. Plaintiff, on behalf of herself and all other Class members, asserts claims for negligence, negligence per se, breach of fiduciary duty, breach of express contract, breach of implied contract, unjust enrichment, and violations of New York General Business Law § 349, and seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

7. Plaintiff Rebecca Krandle is a New York resident. Plaintiff Krandle is a former employee and patient of RHC. She received a letter from RHC notifying her that her PII/PHI was

exposed in the Data Breach. Plaintiff Krandle would not have sought employment or received services from RHC had she known that her PII/PHI would not be adequately safeguarded by RHC.

8. Defendant Refuah Health Center, Inc. is a not-for-profit corporation formed in New York. RHC's principal place of business is located at 728 North Main Street, Spring Valley, New York 10977.

JURISDICTION AND VENUE

9. This Court has personal jurisdiction over RHC because RHC is a corporation formed under the laws of New York and has its principal place of business in New York.

10. Venue is proper in Rockland County because RHC's principal place of business is located in Rockland County.

FACTUAL ALLEGATIONS

Overview of RHC

11. RHC is "a full-service, integrated, multi-specialty healthcare organization with four service sites and a fleet of mobile medical units."¹ The company claims to work "hand-in-hand with patient and provider to ensure that our services meet the needs of our members on the individual level."²

12. In the regular course of its business, RHC collects and maintains the PII/PHI of its patients.

13. RHC provides its patients with its Notice of Privacy Practices. The Notice of Privacy Practices states, "We at Refuah Health Center respect your privacy. This is part of our

¹ *About Refuah Health*, REFUAH HEALTH CENTER, <https://refuahhealth.org/about/> (last accessed May 17, 2022).

² *Why Choose Refuah Health*, REFUAH HEALTH CENTER, <https://refuahhealth.org/about/why-refuah/> (last accessed May 17, 2022).

code of ethics.”³ The notice goes on to state, “We are required by law to maintain the privacy of “Protected Health Information” (“PHI”) about you”⁴

14. Plaintiff and Class members are, or were patients of RHC and entrusted RHC with their PII/PHI.

The Data Breach

15. Between May 31, 2021 and June 1, 2021, an unauthorized individual, or unauthorized individuals, gained access to RHC’s network systems and accessed and acquired certain files on RHC’s computer systems.

16. RHC did not begin to notify government agencies or the public about the data breach until over ten months after the breach, on or about April 29, 2022. The notice that RHC posted to its website states that the information that the cybercriminal extracted from RHC’s network includes “full names and one or more of the following: Social Security numbers, driver’s license numbers, state identification numbers, dates of birth, bank/financial account information, credit/debit card information, medical treatment/diagnosis information, Medicare/Medicaid numbers (which may be identical to Social Security numbers), medical record numbers, patient account numbers, and/or health insurance policy numbers.”⁵

17. RHC’s notice states that its investigation into the Data Breach revealed on March 2, 2022, that PII/PHI related to Plaintiff and Class members “was removed from [its] network in

³ *Notice of Privacy Practices*, REFUAH HEALTH CENTER, https://refuahhealth.org/wp-content/uploads/2016/08/refuah-notice-of-privacy-practice_cmp.pdf (last accessed May 17, 2022).

⁴ *Id.*

⁵ *Notice of Data Security Incident*, REFUAH HEALTH CENTER, <https://refuahhealth.org/wp-content/uploads/2022/04/Refuah-Health-Center-Provides-Notification-of-Information-Security-Incident-to-Affected-Individuals-10279043x7AB84.pdf> (last accessed May 17, 2022).

connection with this incident.”⁶ Despite this, RHC still waited almost two months to tell its patients and former patients that the breach occurred.

18. On June 11, 2021, cybercriminals from the Lorenz ransomware group posted on their dark web site that the group had extracted RHC information.⁷

RHC Knew that Criminals Target PII/PHI

19. At all relevant times, RHC knew, or should have known, that the PII/PHI that it collected was a target for malicious actors. Despite such knowledge, RHC failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff’s and Class members’ PII/PHI from cyber-attacks that RHC should have anticipated and guarded against.

20. It is well known amongst companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers (“SSNs”) and medical information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that “[d]ata breaches are on the rise for all kinds of businesses, including retailers Many of them were caused by flaws in . . . systems either online or in stores.”⁸

21. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2021 report, the healthcare compliance company Protenus found that there were

⁶ *Id.*

⁷ Refuah Health Center “Recently Discovered” a Breach That Was Listed on the Dark Web in June, 2021?, DATABREACHES.NET, <https://www.databreaches.net/refuah-health-center-recently-discovered-a-breach-that-was-listed-on-the-dark-web-in-june-2021/> (last accessed May 17, 2022).

⁸ Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), <https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1>.

758 medical data breaches in 2020, with over 40 million patient records exposed.⁹ This is an increase from the 572 medical data breaches that Protenus compiled in 2019.¹⁰

22. PII/PHI is a valuable property right.¹¹ The value of PII/PHI as a commodity is measurable.¹² “Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks.”¹³ American companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in 2018.¹⁴ It is so valuable to identity thieves that once PII/PHI has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

23. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, SSNs, PII/PHI, and other sensitive information directly on various Internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

⁹ Protenus, *2021 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/resources/2021-breach-barometer> (last accessed May 17, 2022).

¹⁰ Protenus, *2020 Breach Barometer*, PROTENUS.COM, <https://www.protenus.com/resources/2020-breach-barometer> (last accessed May 17, 2022).

¹¹ See Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) (“The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...”).

https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.

¹² See Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market*, MEDSCAPE.COM (April 28, 2014), <http://www.medscape.com/viewarticle/824192>.

¹³ OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD ILIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

¹⁴ IAB Data Center of Excellence, *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), <https://www.iab.com/news/2018-state-of-data-report/>.

24. PHI is particularly valuable and has been referred to as a “treasure trove for criminals.”¹⁵ A cybercriminal who steals a person’s PHI can end up with as many as “seven to ten personal identifying characteristics of an individual.”¹⁶

25. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to \$1,200 to \$1,300 each on the black market.¹⁷ According to a report released by the Federal Bureau of Investigation’s (“FBI”) Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.¹⁸

26. Criminals can use stolen PII/PHI to extort a financial payment by “leveraging details specific to a disease or terminal illness.”¹⁹ Quoting Carbon Black’s Chief Cybersecurity Officer, one recent article explained: “Traditional criminals understand the power of coercion and extortion . . . By having healthcare information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do.”²⁰

¹⁵ See Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAGAZINE (Oct. 20, 2019), <https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon> (“*What Happens to Stolen Healthcare Data*”) (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating “Health information is a treasure trove for criminals.”).

¹⁶ *Id.*

¹⁷ SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAGAZINE (July 16, 2013), <https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market>.

¹⁸ Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), <https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf> (last accessed May 17, 2022).

¹⁹ *What Happens to Stolen Healthcare Data*, *supra* at n.16.

²⁰ *Id.*

27. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that “when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites.”²¹

28. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers’ PII/PHI has thus deprived that consumer of the full monetary value of the consumer’s transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

29. Theft of PII/PHI is serious. The FTC warns consumers that identity thieves use PII/PHI to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person’s name.²²

30. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.²³ According to Experian, one of the largest credit reporting companies in the world, “[t]he research shows that personal information is

²¹ Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) <https://www.jstor.org/stable/23015560?seq=1>.

²² See Federal Trade Commission, *What to Know About Identity Theft*, FEDERAL TRADE COMMISSION CONSUMER INFORMATION, <https://www.consumer.ftc.gov/articles/what-know-about-identity-theft> (last accessed May 17, 2022).

²³ The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.” 16 C.F.R. § 603.2. The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id.*”

valuable to identity thieves, and if they can get access to it, they will use it” to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver’s license or ID; use the victim’s information in the event of arrest or court action.²⁴

31. With access to an individual’s PII/PHI, criminals can do more than just empty a victim’s bank account—they can also commit all manner of fraud, including: obtaining a driver’s license or official identification card in the victim’s name but with the thief’s picture; using the victim’s name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s SSN, rent a house, or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest, resulting in an arrest warrant being issued in the victim’s name.²⁵

32. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.²⁶

33. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to

²⁴ See Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself*, EXPERIAN, <https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/> (last accessed May 17, 2022).

²⁵ See Federal Trade Commission, *Warning Signs of Identity Theft*, IDENTITYTHEFT.GOV <https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft> (last accessed May 17, 2022).

²⁶ Identity Theft Resource Center, *2021 Consumer Aftermath Report*, IDENTITY THEFT RESOURCE CENTER (2021), <https://www.idtheftcenter.org/identity-theft-aftermath-study/> (last accessed May 17, 2022).

demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

34. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, “If I have your name and your Social Security number and you don’t have a credit freeze yet, you’re easy pickings.”²⁷

35. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information “typically leave[] a trail of falsified information in medical records that can plague victims’ medical and financial lives for years.”²⁸ It “is also more difficult to detect, taking almost twice as long as normal identity theft.”²⁹ In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI “to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care.”³⁰ The FTC also warns, “If the thief’s health information is mixed with yours it could affect the medical care you’re able to get or the health insurance benefits you’re able to

²⁷ Patrick Lucas Austin, *‘It Is Absurd.’ Data Breaches Show it’s Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (August 5, 2019), <https://time.com/5643643/capital-one-equifax-data-breach-social-security/>.

²⁸ Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

²⁹ See Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk...*, *supra* at n.19.

³⁰ See Federal Trade Commission, *What to Know About Medical Identity Theft*, Federal Trade Commission Consumer Information, <https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft> (last accessed May 17, 2022).

use.”³¹

36. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services not sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information.
- Sales of medical debt arising from identity theft can perpetuate a victim’s debt collection and credit problems, through no fault of their own.³²

37. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, but it takes some individuals up to three years to learn that information.³³

³¹ *Id.*

³² See Pam Dixon and John Emerson, *The Geography of Medical Identity Theft*, *supra* at n.29.

³³ John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 Journal of Systemics, Cybernetics and Informatics 9 (2019), <http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf>.

38. It is within this context that Plaintiff and Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and the Other Class Members

39. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in RHC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

CLASS ALLEGATIONS

40. This action is brought and may be properly maintained as a class action pursuant to N.Y. C.P.L.R. §§ 901, *et seq.*

41. Plaintiff brings this action on behalf of herself and all members of the following Class of similarly situated persons:

All persons whose PHI/PII was accessed by and disclosed to unauthorized persons in the Data Breach, including all persons who were sent a notice of the Data Breach.

42. Excluded from the Class is Refuah Health Center, Inc. and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge(s).

43. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

44. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. RHC reported to the United States Department of Health and Human Services Office of Civil Rights that approximately 260,740 persons' information was exposed in the Data Breach.

45. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

- a. Whether RHC had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' PII/PHI from unauthorized access and disclosure;
- b. Whether RHC failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' PII/PHI;
- c. Whether an implied contract existed between Class members and RHC, providing that RHC would implement and maintain reasonable security measures to protect and secure Class Members' PII/PHI from unauthorized access and disclosure;
- d. Whether RHC breached its duties to protect Plaintiff's and Class members' PII/PHI; and
- e. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

46. RHC engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and all other Class members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

47. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had her PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by RHC, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

48. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

49. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against RHC, so it would be impracticable for Class members to individually seek redress from RHC's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I **NEGLIGENCE**

50. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

51. RHC owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their PII/PHI in its possession, custody, or control.

52. RHC knew the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. RHC knew of the many data breaches that targeted companies that stored PII/PHI in recent years.

53. Given the nature of RHC's business, the sensitivity and value of the PII/PHI it maintains, and the resources at its disposal, RHC should have identified the vulnerabilities to their systems and prevented the Data Breach from occurring.

54. RHC breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

55. It was reasonably foreseeable to RHC that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

56. But for RHC's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

57. As a result of RHC's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in RHC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II **NEGLIGENCE PER SE**

58. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

59. RHC's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules").

60. RHC's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as RHC, of failing to employ reasonable measures to protect and secure PII/PHI.

61. RHC violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI and not complying with applicable industry standards. RHC's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and stores, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

62. RHC's violation of HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence per se.

63. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

64. The harm occurring as a result of the Data Breach is the type of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

65. It was reasonably foreseeable to RHC that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security

processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

66. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of RHC's violations of harm HIPAA Privacy and Security Rules and Section 5 of the FTCA. Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in RHC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY

67. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

68. Plaintiff and Class members gave RHC their PII/PHI in confidence, believing that RHC would protect that information. Plaintiff and Class members would not have provided RHC with this information had they known it would not be adequately protected. RHC's acceptance and storage of Plaintiff's and Class members' PII/PHI created a fiduciary relationship between RHC and Plaintiff and Class members. In light of this relationship, RHC

must act primarily for the benefit of its patients, which includes safeguarding and protecting Plaintiff's and Class members' PII/PHI.

69. RHC has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII/PHI, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class members' PII/PHI that it collected.

70. As a direct and proximate result of RHC's breaches of its fiduciary duties, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in RHC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT IV
BREACH OF EXPRESS CONTRACT

71. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

72. Plaintiff and Class members and RHC entered into written agreements regarding their medical care and other services that RHC was to provide to Plaintiff and Class members. Plaintiff and Class members paid RHC monies, directly or through an insurance

carrier and provided RHC with their PII/PHI as consideration for these agreements. RHC's Notice of Privacy Practices is evidence that data security was a material term of these contracts.

73. Plaintiff and Class members complied with the express contract when they paid RHC, directly or through an insurance carrier and provided their PII/PHI to RHC.

74. RHC breached its obligations under the contracts between itself and Plaintiff and Class members by failing to implement and maintain reasonable security measures to protect and secure their PII/PHI.

75. RHC's breach of the express contracts between itself, on the one hand, and Plaintiff and Class members, on the other hand directly caused the Data Breach.

76. Plaintiff and all other Class members were damaged by RHC's breach of express contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT V
BREACH OF IMPLIED CONTRACT

77. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

78. In connection with receiving health care services, Plaintiff and all other Class members entered into implied contracts with RHC.

79. Pursuant to these implied contracts, Plaintiff and Class members paid money to RHC and provided RHC with their PII/PHI. In exchange, RHC agreed to, among other things, and Plaintiff understood that RHC would: (1) provide health care or other services to Plaintiff and Class member; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) protect Plaintiff's and Class members PII/PHI in compliance with federal and state laws and regulations and industry standards.

80. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and RHC, on the other hand. Indeed, as set forth *supra*, RHC recognized the importance of data security and the privacy of its patients' PII/PHI in its Notice of Privacy Practices. Had Plaintiff and Class members known that RHC would not adequately protect its patients' and former patients' PII/PHI, they would not have received services from RHC.

81. Plaintiff and Class members performed their obligations under the implied contract when they provided RHC with their PII/PHI and paid RHC for services.

82. RHC breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, and industry standards.

83. RHC's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

84. Plaintiff and all other Class members were damaged by RHC's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face; and (vii) overpayment for the services that were received without adequate data security.

COUNT VI
UNJUST ENRICHMENT

85. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

86. This claim is pleaded in the alternative to the breach of express contract and breach of implied contract claims.

87. Plaintiff and Class members conferred a monetary benefit upon RHC in the form of monies paid for services.

88. RHC accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. RHC also benefitted from the receipt of Plaintiff's and Class members' PII/PHI.

89. As a result of RHC's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

90. RHC should not be permitted to retain the money belonging to Plaintiff and Class members because RHC failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

91. RHC should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VII
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349

92. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

93. New York General Business Law § 349(a) states, "Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."

94. RHC engaged in "business," "trade," or "commerce" within the meaning of N.Y. Gen. Bus. Law § 349(a).

95. Plaintiff and Class members are "persons" within the meaning of N.Y. Gen. Bus. Law § 349(h).

96. RHC makes explicit statements to its patients that their PII/PHI will remain private.

97. RHC's failure to make Plaintiff and Class members aware that it would not adequately safeguard their information while maintaining that it would is a "deceptive act or practice" under N.Y. Gen. Bus. Law § 349.

98. Had Plaintiff and Class members been aware that RHC omitted or misrepresented facts regarding the adequacy of its data security safeguards, Plaintiff and Class members would not have sought services from RHC.

99. Due to the Data Breach, Plaintiff and Class members have lost property in the form of their PII/PHI. Further, RHC's failure to adopt reasonable practices in protecting and safeguarding its patients' PII/PHI will force Plaintiff and Class members to spend time or money to protect against identity theft. Plaintiff and Class members are now at a higher risk identity theft and other crimes. This harm sufficiently outweighs any justifications or motives for RHC's practice of collecting and storing PII/PHI without appropriate and reasonable safeguards to protect such information.

100. As a result of RHC's violations of the N.Y. Gen. Bus. Law § 349, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in RHC's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

101. Pursuant to N.Y. Gen. Bus. Law § 349(h), Plaintiff seeks damages on behalf of herself and the Class in the amount of the greater of actual damages or \$50 for each violation of N.Y. Gen. Bus. Law § 349. Because RHC's conduct was committed willfully and knowingly, Plaintiff and Class members are entitled to recover up to three times their actual damages up to \$1,000.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in her favor and against RHC as follows:

- A. Certifying the Class as requested herein, designating Plaintiff as Class representative, and appointing Plaintiff's counsel as Class Counsel;
- B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;
- C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of herself and the Class, seeks appropriate injunctive relief designed to prevent RHC from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;
- D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;
- E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: May 17, 2022

Respectfully submitted,

/s/ Michael Liskow

Michael Liskow

CALCATERRA POLLACK LLP

1140 Avenue of the Americas, 9th Floor

New York, New York 10036

Phone: (212) 899-1760

Fax: (332) 206-2073

Email: mliskow@calcaterrapollack.com

Anthony L. Parkhill*

Riley W. Prince*

BARNOW AND ASSOCIATES, P.C.

205 West Randolph Street, Ste. 1630

Chicago, IL 60606

Tel: 312-621-2000

Fax: 312-641-5504

aparkhill@barnowlaw.com

rprince@barnowlaw.com

*pro hac vice to be submitted